AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

Claims 1-9.   (Canceled)

10.   (Currently amended) An information processing device <u>for decoding information received from a remote device, the information being encoded with a first key and the first key being encrypted by a second key, the device</u> comprising:

~~a first storage means for storing an encrypted first key encrypted by a second key shared with another device and a decoding means, the first storage means~~ <u>a security unit and a decoding unit, wherein the security unit comprises:</u>

first authentication means for authenticating the decoding ~~means~~ <u>unit</u> and generating a temporary key shared with the decoding ~~means~~ <u>unit</u>;

first encrypting/decrypting means for decrypting the encrypted first key with the second key, and [[for]] <u>then</u> encrypting the first key with the temporary key; and

transmitting means for transmitting the encrypted first key and the temporary key generated by the first authentication means <u>to the decoding unit</u>; <u>and</u>

the decoding ~~means~~ <u>unit</u> ~~comprising~~ <u>comprises</u>:

second authentication means for authenticating the ~~first storage means~~ <u>security unit</u>;

receiving means for receiving the encrypted first key and the temporary key from the ~~first storage means~~ <u>security unit</u>; and

-2-

second ~~encrypting/decrypting~~ <u>decrypting</u> means for decrypting the encrypted first key with the temporary key;

wherein the decoding ~~means~~ <u>unit</u> decodes the information with the first key obtained by the second ~~encrypting/decrypting~~ <u>decrypting</u> means.

11.   (Currently amended) An information processing method <u>for decoding information received from a first device, wherein the information is encoded with an encrypted first key,</u> comprising:

a first storage step of storing ~~an~~ <u>the</u> encrypted first key <u>in a memory of a security unit in a second device, wherein the encrypted first key is</u> encrypted by a second key;

a first authentication step of authenticating a first decoding step and generating a temporary key, the temporary key being shared in the first decoding step;

a first encrypting/decrypting step of decrypting the encrypted first key with the second key, and encrypting the first key with the temporary key;

transmitting the encrypted first key and the temporary key generated in the first authentication step <u>to a decoding unit in the second device</u>;

the first decoding step including a second mutual authentication step of authenticating the first storage step;

receiving the encrypted first key and the temporary key;

a second ~~encrypting/decrypting~~ <u>decrypting</u> step of decrypting the encrypted first key with the temporary key; and

a second decoding step of decoding the information with the first key obtained by the second ~~encrypting/decrypting~~ <u>decrypting</u> step.

12.   (Currently amended) A program providing medium for providing a computer-readable program to cause an information processing device to perform a method for decoding information received from a first device, wherein the information is encoded with an encrypted first key, comprising:

a first storage step of storing ~~an~~ the encrypted first key in a memory of a security unit in a second device, wherein the encrypted first key is encrypted by a second key;

a first authentication step of authenticating a first encrypting/decrypting step and generating a temporary key, the temporary key being shared in the first encrypting/decrypting step;

the first encrypting/decrypting step including ~~encrypting/decrypting~~ decrypting the encrypted first key with the second key and including encrypting the first key with the temporary key;

transmitting the encrypted first key with the temporary key to a decoding unit in the second device;

the program causing a decoding means to execute processing comprising:

a second authentication step of authenticating the first storage step;

receiving the encrypted first key with the temporary key from the first storage step;

a second ~~encrypting/decrypting~~ decrypting step of decrypting the encrypted first key with the temporary key; and

a third encrypting/decrypting step of decoding the information with the first key obtained by the second encrypting/decrypting step.

Claims 13-71.   (Canceled)